References

[CHH16] Michael Colesky, Jaap-Henk Hoepman and Christiaan Hillen. A critical analysis of privacy design strategies. In *2016 International Workshop on Privacy Engineering – IWPE'16*, pages 33–40. San Jose, CA, USA, May 26 2016.

[CHR+16] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska and Peter Schwabe. From 5-pass MQ-based identification to MQ-based signatures. In *Advances in Cryptology – ASIACRYPT 2016* (edited by Jung Hee Cheon and Tsuyoshi Takagi), volume 10032 of *LNCS*, pages 135–165. Springer, 2016. doi: 10.1007/978-3-662-53890-6_5.

[HHJ16] Marit Hansen, Jaap-Henk Hoepman and Meiko Jensen. Towards measuring maturity of privacy-enhancing technologies. In *Annual Privacy Forum (APF 2015)*, LNCS9484, pages 3–20. 2016.

[HK16] J.-H. Hoepman and Stefan Katzenbeisser (editors). *ICT Systems Security and Privacy Protection. 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30 - June 1, 2016, Proceedings*, volume 471 of *IFIP Advances in Information and Communication Technology*. Springer, 2016.

[HRS16a] Andreas Hülsing, Joost Rijneveld and Peter Schwabe. ARMed SPHINCS – computing a 41KB signature in 16KB of RAM. In *Public Key Cryptography – PKC 2016* (edited by Giuseppe Persiano and Bo-Yin Yang), volume 9614 of *LNCS*, pages 446–470. Springer, 2016. doi:10.1007/978-3-662-49384-7_17.

[HRS16b] Andreas Hülsing, Joost Rijneveld and Fang Song. Mitigating multi-target attacks in hash-based signatures. In *Public Key Cryptography – PKC 2016* (edited by Giuseppe Persiano and Bo-Yin Yang), volume 9614 of *LNCS*, pages 387–416. Springer, 2016. doi: 10.1007/978-3-662-49384-7_15.

[LEH16a] Wouter Lueks, Maarten Everts and Jaap-Henk Hoepman. Revocable privacy: Principles, use cases, and technologies. In *Annual Privacy Forum (APF 2015)*, LNCS9484, pages 124–143. 2016.

[LEH16b] Wouter Lueks, Maarten Everts and Jaap-Henk Hoepman. Vote to link: recovering from misbehaving anonymous users. In *Workshop on Privacy in the Electronic Society (WPES 2016)*, pages 111–122. Vienna, Austria, October 24 2016. doi:https://doi.org/10.1145/2994620.2994634.

[MRB16] Pedro Maat C. Massolino, Joost Renes and Lejla Batina. Implementing complete formulas on weierstrass curves in hardware. In *Security, Privacy, and Applied Cryptography Engineering: 6th International*

Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings, pages 89–108. Springer International Publishing, 2016. ISBN 978-3-319-49445-6. doi:10.1007/978-3-319-49445-6_5.

[RCB16] Joost Renes, Craig Costello and Lejla Batina. Complete addition formulas for prime order elliptic curves. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, pages 403–428. 2016. doi:10.1007/978-3-662-49890-3_16.

[RSSB16] Joost Renes, Peter Schwabe, Benjamin Smith and Lejla Batina. μkummer: Efficient hyperelliptic signatures and key exchange on microcontrollers. In *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, pages 301–320. 2016. doi: 10.1007/978-3-662-53140-2_15.

[SS16] Peter Schwabe and Ko Stoffelen. All the AES you need on Cortex-M3 and M4. In *Selected Areas in Cryptography – SAC 2016* (edited by Roberto Avanzi and Howard Heys), LNCS. Springer, 2016.

[Sto16a] Ko Stoffelen. Instruction scheduling and register allocation on ARM Cortex-M. In *Software performance enhancement for encryption and decryption, and benchmarking – SPEED-B*. October 2016.

[Sto16b] Ko Stoffelen. Optimizing S-box implementations for several criteria using SAT solvers. In *Fast Software Encryption* (edited by Thomas Peyrin), volume 9783 of *LNCS*, pages 140–160. Springer, 2016. doi: 10.1007/978-3-662-52993-5.

[UW16] Sander Uijlen and Bas Westerbaan. A kochen-specker system has at least 22 vectors. *New Generation Computing*, 34(1-2):3–23, 2016.

[WW16] Abraham Westerbaan and Bas Westerbaan. A universal property for sequential measurement. *Journal of Mathematical Physics*, 57(9):092203, sep 2016. doi:10.1063/1.4961526.